COGNITA

Data Retention Policy

Switzerland

INTERNATIONAL SCHOOL
ZURICH NORTH

KEY FACTS:

Policy Objective

This policy provides guidance in respect of data protection and the retention of personal data within the Cognita group.

Scope

This policy applies to all Cognita Swiss companies and Cognita employees, and all workers who are made aware of this policy.

1 INTRODUCTION

1.1 This Personal Data Retention Policy sets out the rules and procedures around the retention of personal data in those companies which are within the Cognita group in Switzerland (together "**Cognita**") and determines how long you should be keeping certain categories of personal data.

1.2 Please make sure that you read this policy in conjunction with Cognita's Data Protection Policy.

1.3 This policy applies to all Cognita employees and workers who are made aware of this policy. Third parties may also be asked to adhere to this policy. Any breach of this policy may result in disciplinary action / termination of the provision of services by Cognita as appropriate.

1.4 This policy does not form part of any employee's contract of employment and may be amended at any time.

2 AIM OF THIS POLICY

2.1 Article 5(1)(e) of the General Data Protection Regulation ("**GDPR**") requires that personal data shall be kept in a form which permits identification of individuals for no longer than is necessary. Therefore, the key aim of this policy is to set out Cognita's rules governing for how long specific types of personal data should be kept.

2.2 Article 5(1)(f) of the GDPR requires that personal data must be processed in a manner that ensures appropriate security of personal data, using appropriate technical or organisational measures. Another aim of this policy is to guide you on appropriate measures around retaining and destroying hard copy documents securely.

3 WHAT IS NOT COVERED IN THIS POLICY?

3.1 This policy relates to records, documents or information which capture personal data in any way. Nonetheless, those records, documents or information might be sensitive in another way (for example, legally, commercially or financially sensitive) and you may need to refer to a policy which is specific to that information. In the absence of any policies, we encourage you to adopt a common sense approach when deciding how long to store the information and when to destroy it.

3.2 Further information about the definition of personal data is set out in the Data Protection Policy. If you are not sure whether a certain piece of information is personal data, please check the Data Protection Policy which provides some more information about what personal data is. If you are still not sure, then please speak to your Data Protection Co-ordinator.

3.3 For further information regarding your responsibilities relating to IT security, please see our IT Policies.

4 WHO CAN I SPEAK TO ABOUT THIS POLICY?

Cognita's Data Protection Officer

4.1 Cognita has appointed a Data Protection Officer (**"DPO"**) who is responsible for overseeing compliance with Data Protection Laws and with this policy. That post is held by Jayne Pinchbeck, General Counsel, DPO@cognita.com. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

Data Protection Co-ordinators

4.2 A Data Protection Co-ordinator ("**DPC**") has been designated for the School Community Partners. In addition, a school DPC has been designated for each school. Please contact the Data Protection Team via DPO@cognita.com if you have any queries or concerns relating to this policy.

5 RETENTION PERIODS

5.1 With the exception of paragraph 6 below, you must make sure that personal data is retained for the period of time indicated in the Retention Schedule which is annexed to this policy.

5.2 If you think there is a particular category of personal data missing from the Retention Schedule, please speak to your Data Protection Co-ordinator to find out what is the appropriate retention period.

6 RETENTION OF DATA BEYOND THE RETENTION PERIOD

Where data should be retained indefinitely

6.1 If you receive notice of any legal proceedings or legal action (or potential legal action), government or regulatory investigation or complaints or claim against or involving Cognita and/or any of its schools (for example, a complaint made by a parent or a grievance raised by an employee), then you should flag and retain all data which may be relevant to that issue. **Please do not destroy that data**. If you are ever unsure about which data you should be retaining and which data you should be destroying in accordance with the Retention Schedule, please speak to your Data Protection Co-ordinator.

6.2 The legal team will work with you in determining what information is relevant for the case and what isn't. As a general rule (and as set out in the Retention Schedule), once the claim has concluded (e.g. a judgment has been given by the court or the claim has settled), then information about the claim should be kept for a further 6 years before being destroyed.

6.3 In certain circumstances, you may want to keep a record of certain files or information that you have securely deleted. For example, when you destroy a child protection file, you may feel it is appropriate to keep a note of this (and securely store that note) just in case the pupil ever makes an enquiry. By the same measure, you may want to keep a record of files which you have not destroyed, for example, where there are ongoing or likely legal proceedings which requires you to keep records for longer than the standard retention periods (see paragraph 6.1 above).

7 TRANSFERRING PUPIL FILES

7.1 Please see the Retention Schedule about transferring pupil files.

8 ARCHIVING PERSONAL DATA

8.1 Archiving personal data is not the same as destroying it. If you are archiving personal data, you will need to ensure that personal data is only archived within the retention periods set out in the Retention Schedule.

Hard (or physical) copies

8.2 When destroying paper documents containing personal data, please make sure they are shredded with a cross-cut shredder or placed in a secure, confidential document shredding box.

Hard drives

8.3 Once obsolete, computer hard drives and portable media previously used by you or any third party suppliers should be handed to the IT Team to be properly wiped, and where so appropriate, destroyed.

Email retention and deletion

8.4 Cognita intends to adopt a group wide email retention policy in the near future. When adopted, emails will be automatically deleted by the IT Team after e.g. 5 years (subject to the rest of this paragraph).

8.5 Once Cognita adopts its automatic email retention period, it will be possible to set up a folder in your inbox to save emails to be kept beyond the retention period and you will be guided about when the automatic retention period will become effective and how to archive your emails via the IT Team in due course. In the meantime, you should delete any emails that you do not need and archive any emails you need to keep. It is up to you what method you use to archive emails as long as you are adopting a sensible and organisational approach. For example, you may have an isolated ongoing issue with a particular member of staff or pupil (say, a complaint or grievance). You should create a folder in your inbox which has, all in one place, all emails relating to that issue so they are easy to locate.

8.6 Please note, however, that the option to archive your emails (extending the automatic retention policy) will not allow you to routinely save emails into this folder (and the IT Team in the School Support Centre will be monitoring this folder to check in accordance with our Digital Safety Policy): only those emails which you need for longer periods. You may also want to think about other ways of keeping those emails: for example, if they relate to an ongoing case or claim, you should liaise with the legal team about whether they have a separate bundle which means you do not have to hold on to the emails yourself. Or perhaps you need the attachments in the email, but not necessarily the email itself, in which case you should save the attachments in your personal folder and delete the email itself when no longer needed.

9 DELETING DATA WHICH IS OUT OF DATE

9.1 Article 5(1)(d) of the GDPR requires that personal data shall be accurate and, where necessary, kept up to date. When you have information which you know is out of date then you should be securely deleting that data in accordance with this policy.

10 CHANGES TO THIS POLICY

10.1 We reserve the right to change this policy at any time. Where appropriate, we will notify you about those changes.

DATA PROTECTION RETENTION SCHEDULE

MEMBERS OF STAFF			
This includes all employees, permanent members of staff and, where relevant, supply teachers and self-employed contractors. In relation to those people who are engaged by the school or head office on a short term basis, you will probably be collecting a limited amount of information on these people, particularly if they are engaged via a recruitment agent to fill a vacancy for a short period. Please exercise your discretion regarding how long to keep personal information about this type of person. If a shorter retention period is more appropriate (say, 6 months) then please delete information about this person before the end of that period.			
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Suggested Retention Period** (retention periods will depend on the specific circumstances of the case)
1	List of all members of staff and employees and dates of employment	N/A	While the employment relationship continues to be in force and up to 5 years after termination of the same.
2	Employee offer letters, confirmation of employment letters, written particulars of employment, contracts of employment and changes to the terms and conditions	Act on Federal Data Protection (nFADP)	While the employment relationship continues to be in force and up to 6 years afterwards.
3	Training records agreements	Act on Federal Data Protection (nFADP)	While the employment relationship continues to be in force and up to 6 years afterwards.
4	Personnel files (including all records relating to promotions, demotions, grievance procedures, resignation or termination letters)	N/A	While the employment relationship continues to be in force and up to 5 years after termination of the same.
5	Staff sickness records	N/A	While the employment relationship continues to be in force and up to 5 years after termination of the same.
6	Job descriptions and performance goals	N/A	While the employment relationship continues to be in force and up to 5 years after termination of the same.
7	Current bank details	N/A	While the employment relationship continues to be in force and up to 1 year after termination of the same (unless a claim has been filed against the company, in which case this term can be extended for so long as the subsequent employment process is ongoing).

8	Pension records (i.e. the record of the pensionable service and the pension provider)	N/A	While the employment relationship continues to be in force and up to 5 years after termination of the same.
9	Information on benefits per member of staff/employee	N/A	6 years from the end of the financial year in which they were collected.
10	Pre-employment vetting records (job applications, CVs and interview records)	N/A	Up to 6 months after the vetting decision is made (longer periods might be agreed with the applicant; however, the risks arising from the use of outdated data must be carefully considered).
10(a)	Supplementary guidance on pre-employment vetting records: where the applicant is unsuccessful, and you wish to retain names in the Cognita Talent Pool for future vacancies please make sure you have advised unsuccessful candidates of your intention to do so and give them the opportunity to have their details removed from the file. If you intend to keep an unsuccessful applicant on the Cognita Talent Pool for longer than 6 months, please ensure you have obtained the permission of the applicant. Please make sure that, during the recruitment process, you only collect the information that you need. Please give consideration to the sort of information that is obtained as part of recruitment, particularly as it goes towards the employee file if the applicant is successful.		
11	Criminal checks records (being 1. the DBS number 2. overseas disclosure and barring checks 3. any confirmation or report that the applicant is not barred and 4. any records of the conversation you have had with the applicant about any convictions and 5. any risk assessments).	N/A	We can keep a record that a criminal record check has been completed and is negative. Retention of records relating to criminal offences can only be retained when required by Law e.g. required for safeguarding. On top of this, only documents relating to sexual assaults should be retained. These records should be kept until the new checks (for renewal) take place.
12	Records resulting from warnings (including, where the warning is written, the written warning itself)	N/A	It will depend very much on the nature of the warning (pure employment disciplinary or even subject to be considered, tax infringement or criminal offense). However, and due to the fact that the warning will take place within an employment relationship, as a general rule the retention period will be while the employment relationship continues to be in force and up to 6 years afterwards
13	Immigration checks (being work permits)	N/A	Where the applicant is unsuccessful, no later than 6 months from the decision to reject the applicant. Where the applicant is successful, 6 years after the termination of the working relationship.
14	Records relating to accidents / injury at work	N/A	5 years from the time of the accident and/or since the final scope of injuries suffered by the employee is known.
15	Working time opt-out agreements	Labour infringements and sanctions Act	While the working relationship continues to be in force and up to 4 years after termination of the same.

16	Records to show compliance with the Statute of Workers Rights	Act on Federal Data Protection (nFADP)	While the working relationship continues to be in force and up to 4 years after termination of the same.
17	Annual leave records (including maternity and parental leave records)	Act on Federal Data Protection (nFADP)	While the employment relationship continues to be in force and up to 5 years after termination of the same.
18	Payroll and wage records (including PAYE records, maternity pay and work schemes)	Act on Federal Data Protection (nFADP)	While the employment relationship continues to be in force and up to 5 years after termination of the same.
19	Death benefit nomination and revocation forms	N/A	While employment continues and/or up to 5 years after payment of benefit.
20	Staff emails	N/A	While the working relationship continues to be in force and up to 5 years after termination of the same.

PUPILS			
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**
1	Pupil applicants who did not enrol	N/A	All files to be destroyed once an ultimate decision is made.
2	Special Educational Needs files, Education, provision maps (or equivalent), and professional reports in relation to the child's educational or medical needs (including reports by an educational psychologist, specialist	N/A	6 years from the time the pupil left school.

	teacher, speech and language therapist, occupational therapist or medical practitioner)			
3	Records relating to accidents / injury in school	Act on Federal Data Protection (nFADP)	5 years from the time of the accident and/or since the final scope of injuries suffered by the pupil are known.	
4	Parental permission slips (e.g. for school trips, activities or sessions where getting parental permission is appropriate) where there has been no major incident.	N/A	The relevant academic year.	
5	Pupil emails	N/A	During the academic relationship between the pupil and the school, plus one additional academic year after the pupil has left the school (termination of the relationship).	
6	**Pupil education records** which include the following about the pupil (although this is not an exhaustive list):	N/A	Paper	Electronic

	• progress reports; • medical records of pupils with medical conditions and details for the administration of medicines; • internal examination results; • external examination certificates; • record of academic achievement; • letters and communication between school and parent; • report card; • behaviour records; • attendance record; • attendance register • admissions register • reports from external professionals and agencies (although please see below if the report relates to a child protection issue); • Health and Care Plans and • exclusion records and copies of letters.		6 years from the time the pupil left the school.	6 years from the time the pupil left the school, please then delete any electronic information relating to the pupil (except for alumni data on which please see below).
6(a)	Supplementary guidance on **pupil education records**: for pupils where a safeguarding concern has been raised, records must be kept separately from the pupil education record and please see below for information relating to child protection issues. Also, if the child has special educational needs, please see item 2 above.			
7	Alumni data: name, email address and home address of pupil	N/A	This should be kept indefinitely , although this list will need to be revisited periodically (we recommend annually) to check whether very historic alumni data should be deleted and whether anyone has requested to be removed from this list. Please make sure that you keep this list accurate and up to date. Please make sure that you only use pupil alumni data for the limited purpose of updating them on current school news, future events or other appropriate updates.	

Personal Data Retention Policy

CHILD PROTECTION			
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**
1	Child protection file (which contains the cover sheet, chronology, cause for concern forms (possibly with body maps).	N/A	6 years from the time the pupil left the school.
2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded.		Personal data processed by a whistleblowing scheme should be delete immediately afterwards or, the latest, within two months upon completion of the investigation of the facts alleged in the report. This period should be limited to the management of the necessary internal audit measures and, at the most, to the management of the judicial proceedings arising from the investigations carried out.

PARENTS (POTENTIAL CUSTOMERS OR EXISTING CUSTOMERS)			
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**
1	Parent applicants or enquirers where their child does not end up enrolling with the school	N/A	2 years after the date in which the application is closed.
2	Contact details of parents	N/A	If the contact details will be used for marketing purposes, the retention period differs depending on if the parent is a prospective parent or existing parent. If the prospective parent has given consent to ongoing marketing at the enquiry/application stage then 4 years after the date of the application or initial enquiry or last communication from the prospective parent. If the parent is an existing customer, and you wish to continue marketing to the parent, you may keep this information indefinitely, provided that in all communications the parent is given the opportunity to withdraw their consent. The list of existing customers who receive marketing communications will need to be revisited periodically (we recommend annually) particularly when the child has left the school. This is to check

			whether very historic parent alumni data should be deleted and whether anyone has requested to be removed from this list. Please make sure that you keep this list accurate and up to date.
3	Other personal information about parents (including the parent contract, invoices and the parents' financial information)	N/A	Parents' contracts and invoices can be retained for 6 years from the time the pupil left the school.

COMPLAINTS AND LITIGATION			
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**
1	Any information relating to a complaint (whether real or potential) made by a pupil, parent and/or guardian or member of public.	N/A	While the academic relationship continues to be in force and up to 5 years after termination of the same.
2	Records relating to pending, threatened or reasonably anticipated litigation, government investigation, or other claim.	N/A	Please consult the legal team on this. All records should be kept during the period in which the litigation, investigation complaint or claim is contemplated, pending or threatened and until final disposition of the matter (i.e. after a court judgment or final settlement) and then for a period of 6 years after that.

CCTV FOOTAGE			
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**
1	Video recordings from surveillance cameras	Act on Federal Data Protection (nFADP)	Video recording from surveillance cameras should be erased on a monthly basis. Please note that you may need to retain information for a longer period, where a law enforcement body is investigating a crime and ask for it to be preserved, to give them opportunity to view the information as part of an active investigation. Please consult the legal team if you intend to keep CCTV footage for longer.

SUPPLIERS OR CONTRACTORS			
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**
1	Visitor and/or contractor signing-in books	N/A	While the service relationship with the contractor/supplier continues to be in force and up to 5 years after termination of the same or in the case of parents visiting the school, up to 5 years after their visit.

Personal Data Retention Policy

Ownership and consultation	
Document sponsor (role)	Europe CEO
Document author (name)	General Counsel
Specialist Legal Advice	
Consultation	Data Protection Committee

Compliance	
Compliance with	Local legislation

Document application	
Group Wide	Switzerland only

Version control	
Version	1
Implementation date	01/05/2025
Review date	01/05/2026

Related documentation	
Related documentation	Data Protection Policy